Das „S“ in IoT steht für Sicherheit ;-)

AKIS-42 / 02.06.2021

Ihr Referent

Frank Ewert

CEH *– Certified Ethical Hacker*
MCP *– Microsoft® certified Professional*
IMC *– Internet Medien Coach*

Security Evangelist
Stellv. Vorstand Verein Sicheres Netz hilft e.V.

Internet of things is …

when your toaster mines bitcoins to pay off its gambling debts to the fridge

Was ist das „Internet of Things“?

Das **Internet of Things (IoT)** - *auf Deutsch "Internet der Dinge"* - bezeichnet ein System von miteinander vernetzten Maschinen, Anlagen und Geräten über und mit dem Internet.

Internetofthings.de – Sebastian Human

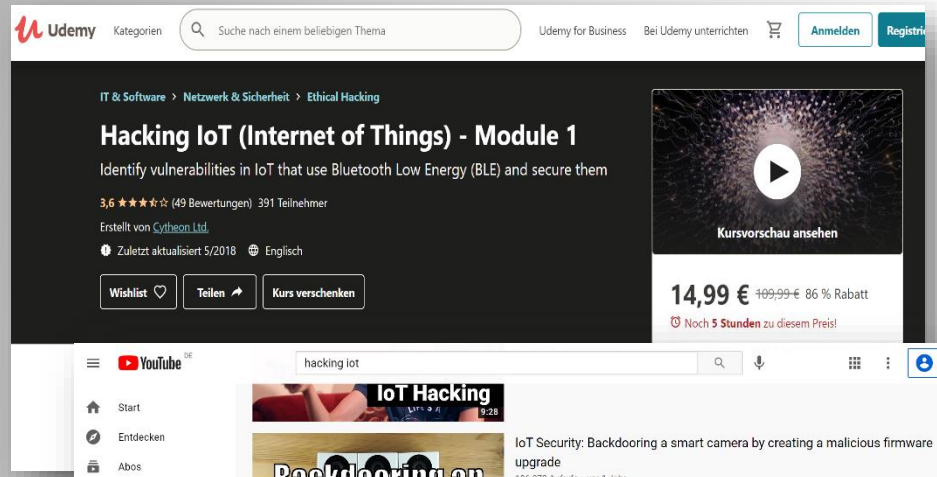
Heutzutage wird das IoT oft mit den gesamten „Smart…“-Objekten* gleichgesetzt, auch wenn diese nur eine Teilmenge daraus bilden.

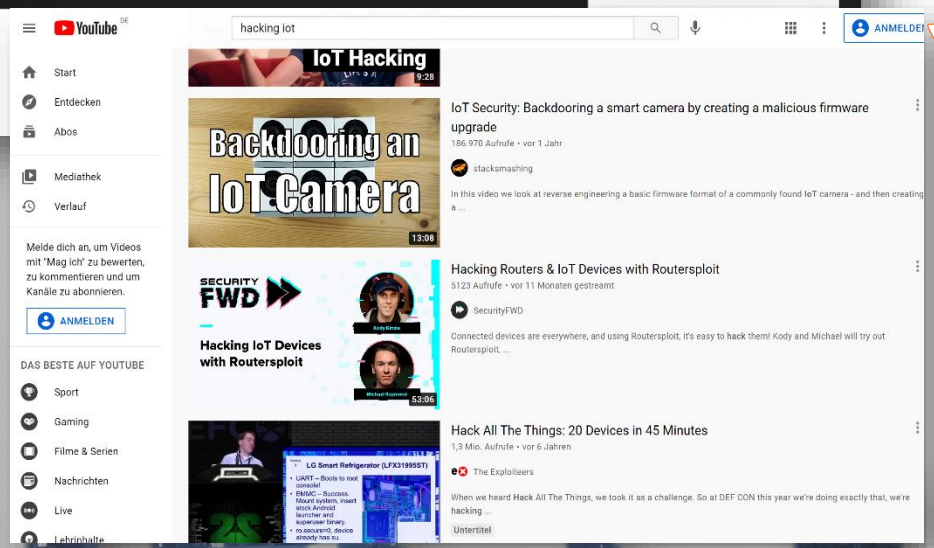
Da die Preise für diese Einheiten - bspw. durch billige China-Importe - deutlich gesunken sind, die **DIY-** (**D**o **I**t Yourself) / **Maker-Szene** großen Gefallen an IoT-Projekten gefunden hat und letztlich der Faktor Sicherheit stark vernachlässigt wird, erfreut sich auch die Hacker-Community am Internet der Dinge ;-)

* Der Teil mit einer mehr industriellen Ausprägung firmiert deshalb auch oft unter ***IIoT***.

Internet of things- Hacks

… und es werden mehr …



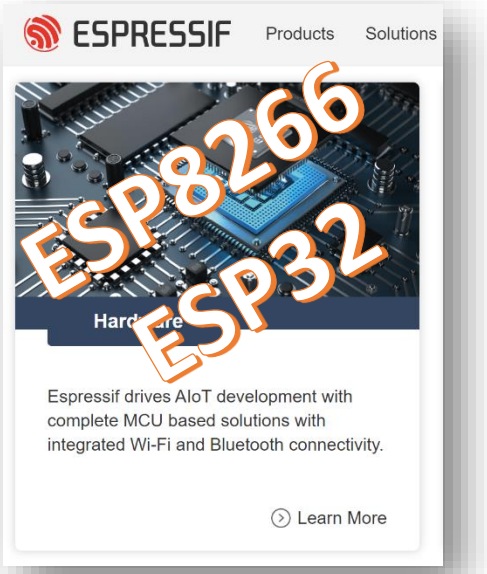


Hacking-Kurs
- ab 14,99 €

YouTube-How Tos
- Backdooring
- Exploiting uvm.

Vorab Kurzinfo: Chips und Boards fürs IoT

In vielen der auf dem Markt und im DIY-Bereich erhältlichen IoT-Einheiten verbergen sich meist nur wenige verschiedene Basissystem/ Chips, abhängig vom Anwendungseinsatz kristallisieren sich folgende Systeme oder deren Derivate heraus:



www.espressif.com

ESPRESSIF

Gute Infos zu ESPs unter
https://randomnerdtutorials.com/

ESP8266 Series Modules

32-bit MCU & 2.4 GHz Wi-Fi

- ESP8266 embedded, Xtensa® single-core 32-bit LX6 microprocessor, up to 160 MHz
- +19.5 dBm output at the antenna ensures a good physical range
- Sleep current is less than 20 µA, making it suitable for battery-powered and wearable-electronics applications
- Peripherals include UART, GPIO, I2C, I2S, SDIO, PWM, ADC and SPI
- Fully certified with integrated antenna and software stacks

ESP32 Series Modules

32-bit MCU & 2.4 GHz Wi-Fi & Bluetooth/Bluetooth LE

- ESP32 embedded, two or one Xtensa® 32-bit LX6 microprocessor(s) with adjustable clock frequency, ranging from 80 MHz to 240 MHz
- +19.5 dBm output power ensures a good physical range
- Classic Bluetooth for legacy connections, also supporting L2CAP, SDP, GAP, SMP, AVDTP, AVCTP, A2DP (SNK) and AVRCP (CT)
- Support for Bluetooth Low Energy (Bluetooth LE) profiles including L2CAP, GAP, GATT, SMP, and GATT-based profiles like BluFi, SPP-like, etc
- Bluetooth Low Energy (Bluetooth LE) connects to smart phones, broadcasting low-energy beacons for easy detection
- Sleep current is less than 5 µA, making it suitable for battery-powered and wearable-electronics applications
- Peripherals include capacitive touch sensors, Hall sensor, SD card interface, Ethernet, high-speed SPI, UART, I2S and I2C
- Fully certified with integrated antenna and software stacks

Quelle: https://www.espressif.com/en/products/modules (Abruf am 30.05.2021)

Zwischenbetrachtung: Sicherheit ≠ Sicherheit

Generell dreht sich beim Thema **Sicherheit** im IT-Umfeld alles um Schutz gegen (Cyber-)Angriffe und für den Datenschutz – kurz **C I A**!

Gemeint sind dabei:

C	onfidentiality	(Vertraulichkeit)
I	ntegrity	(Integrität)
A	vailability	(Verfügbarkeit)

Wenn man mit Sensoren/ Aktoren oder mit einer Hausautomation arbeitet, dann bekommt Sicherheit aber auch eine weitere Bedeutung denn

was passiert bei Störung/ Ausfall der Einheit?

Der englischsprachige Raum unterscheidet deshalb generell in

Security* and *Safty

Wir belassen es heute bei Security…

Top 10 Web Application Security Risks

A1:2017-Injection: Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

A2:2017-Broken Authentication: Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

A3:2017-Sensitive Data Exposure: Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

A4:2017-XML External Entities (XXE): Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

A5:2017-Broken Access Control: Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

A6:2017-Security Misconfiguration: Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.

A7:2017-Cross-Site Scripting XSS: XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

A8:2017-Insecure Deserialization: Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

A9:2017-Using Components with Known Vulnerabilities: Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

A10:2017-Insufficient Logging & Monitoring: Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

Die OWASP* Top 10 IoT

Das OWASP stellt im IT-Sektor (meist) jährlich eine **Top 10 der verbreitetsten Sicherheitsrisiken** zusammen. Gedacht ist diese Liste primär für Sicherheitsfachleute und Entwickler, um ihr Augenmerk für diese Lücken zu schärfen.

* **O**pen **W**eb **A**pplication **S**ecurity **P**roject (Non-Profit Organisation)
https://owasp.org/
https://owasp.org/www-project-top-ten/

Die OWASP* Top 10 IoT

Das OWASP stellt im IT-Sektor (meist) jährlich eine **Top 10 der verbreitetsten Sicherheitsrisiken** zusammen. Gedacht ist diese Liste primär für Sicherheitsfachleute und Entwickler, um ihr Augenmerk für diese Lücken zu schärfen.

Das Teilprojekt **OWASP IoT** hat 2014 und 2018 jeweils eine Top 10 veröffentlich – **mit nahezu gleichem Inhalt**.. Allerdings unterscheiden sich die Standardlisten der PC-Welt in der Regel auch immer nur geringfügig und haben auch viele Parallelen zu den IoT-Listen…

Im heutigen Vortrag können wir gemeinsam leider nur ein paar der Punkte auszugsweise beleuchten, aber dafür hoffe ich diese anschaulich nahezubringen ;-)

* **O**pen **W**eb **A**pplication **S**ecurity **P**roject (Non-Profit Organisation)
https://owasp.org/
https://owasp.org/www-project-top-ten/

TOP 9 – Unsichere Grundeinstellung

Viele Anwender freuen sich wenn Sie auf einer der üblichen Shoppingplattformen für wenig Geld „etwas smartes für Zuhause“ erworben haben…

- 3er-Set WLAN-Steckdosen ür Alexa Voice Service
- **WiFi-kompatibel:** unterstützt WLAN-Standards IEEE 802.11b/g/n (2,4 GHz)
- **Kompatibel mit Alexa Voice Service von Amazon:** Geräte per Echo-Lautsprecher und Sprachbefehl ein- und ausschalten
- **Zugriff von unterwegs:** weltweite App-Steuerung per Internet
- **Kostenlose App** für iOS und Android, erhältlich im App Store und bei Google Play: für Steuerung, Timer-Funktionen und Strom-Messung
- **Zeitschaltuhr-Funktion:** automatische Aktivierung und Deaktivierung nach einstellbarem Zeitplan
- Timer-Funktion bis max. 23 Stunden 55 Minuten Laufzeit: in 5-Minuten-Schritten einstellbarer Countdown schaltet die Steckdose automatisch aus
- **Abwesenheits-Modus:** schalten Sie Lichter & Co. jederzeit ein und aus, täuscht Anwesenheit vor
- **App misst den Stromverbrauch** zuverlässig ab einem Verbrauch von 5 Watt: Milliampere, Volt, Watt, kW/h Tageswert, kW/h Gesamtwert
- Status-LED zeigt Verbindungsqualität
- Einfache Bedienung
- Steckdose belastbar bis 3.680 Watt
- Maximale Stromstärke: 16 A
- Maße: je 54 x 54 x 59 mm, Gewicht: 91 g
- **3 WLAN-Steckdosen inklusive deutscher Anleitung** - Wlansteckdose - Außerdem relevant oder passend zu: Funk, Smart, Apple, Dimmer, Energie, Stecker, Monitor, Elesion, Schalter, Smarthome, Strommessung, Energiezähler, Energiekosten, Bedienungsanleitung
- EAN: 4

★★★★★

Top-Kundenmeinungen!
Über 90% der Käufer urteilen:

- Ausgezeichnet
- Sehr preiswert
- Kaufempfehlung
- Sehr leicht bedienbar
- Sehr innovativ

BESTSELLER

statt € 44,97
39,99*
Sie sparen € 4,98 (11 %).
€ 13,33 pro WLAN-Steckdose.

TOP 9 – Unsichere Grundeinstellung

Damit die Geräte von jedem eingerichtet und bedient werden können steht **Bequemlichkeit statt Sicherheit** im Fokus.

Die Anwender haben schnell ein Erfolgserlebnis und sind tatsächlich auch nach wenigen Minuten in der Lage „weltweit“ ihre Neuerwerbung zu bedienen.

In kaum einer Bedienungsanleitung (sofern diese beigefügt und nicht erst über einen Downloadlink noch geladen werden muss) steht ein Passus, das die gewählten **Grundparameter zur eigenen Sicherheit angepasst werden sollten**…

Schauen wir uns einmal gemeinsam an was es bedeutet die Grundeinstellung einer Gebäudeautomation bzw. dessen Dashboards unverändert zu lassen…

TOP 7 – Datentransfer/-speicherung

Sinn von IoT ist die **einfache Verbindung** diverser Komponenten. Leider nehmen einige Anbieter „einfache Verbindung“ zu wörtlich!

So werden **Daten unverschlüsselt übertragen oder abgespeichert**. Auch die Speicherung von Zugangsdaten in einer Hersteller-Cloud „um die Einrichtung weiterer Geräte zu erleichtern“ ist nicht ganz unproblematisch…

Im IoT-Bereich haben sich, je nach Anwendungsfeld, unterschiedliche Übertragungswege und Protokolle etabliert.

Verbindungen: **WLAN**, ZigBee, Z-Wave, BlueTooth/ BLE, LoRaWAN, EnOcean, NFC/RFID, ua.

Protokolle: HTTP, **MQTT**, CoAP, IFTTT ua.

Viele davon bieten sowohl unverschlüsselten wie auch verschlüsselten Zugriff an – sofern man das weiß…

MQTT – Message Queuing Telemetry Transport

Publisher

Broker

Subscriber

MQTT – Message Queuing Telemetry Transport

ESP32 Pico
auf Developerboard

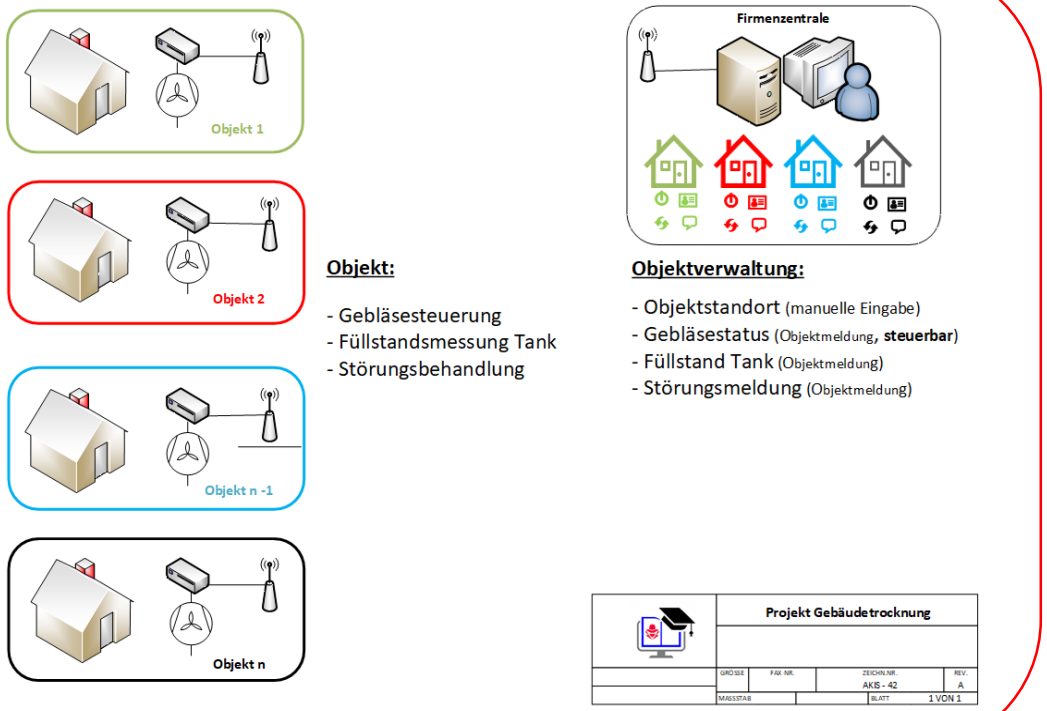
Publisher

Raspberry Pi 3B
Mosquitto-Server

Broker

Raspberry Pi 3B
Node-Red mit DashBoard

Subscriber



Kurze Zwischenfrage:

Handelt es sich hierbei um eine IoT-Lösung?

Projekterläuterung:

Für eine Gebäudetrocknungsfirma werden intelligente Vor-Ort-Einheiten benötigt die:

- ***Stand-Alone arbeiten***
- ***per SMS Kontakt zur Firmenzentrale halten***
- ***Steuerung des Gebläses manuell/ per SMS***
- ***Statusmeldungen versenden/ empfangen***
- ***Füllstand eines Tanks überwachen/melden***
- ***Störungsmeldungen absetzen***

TOP 4 – Updatefunktion

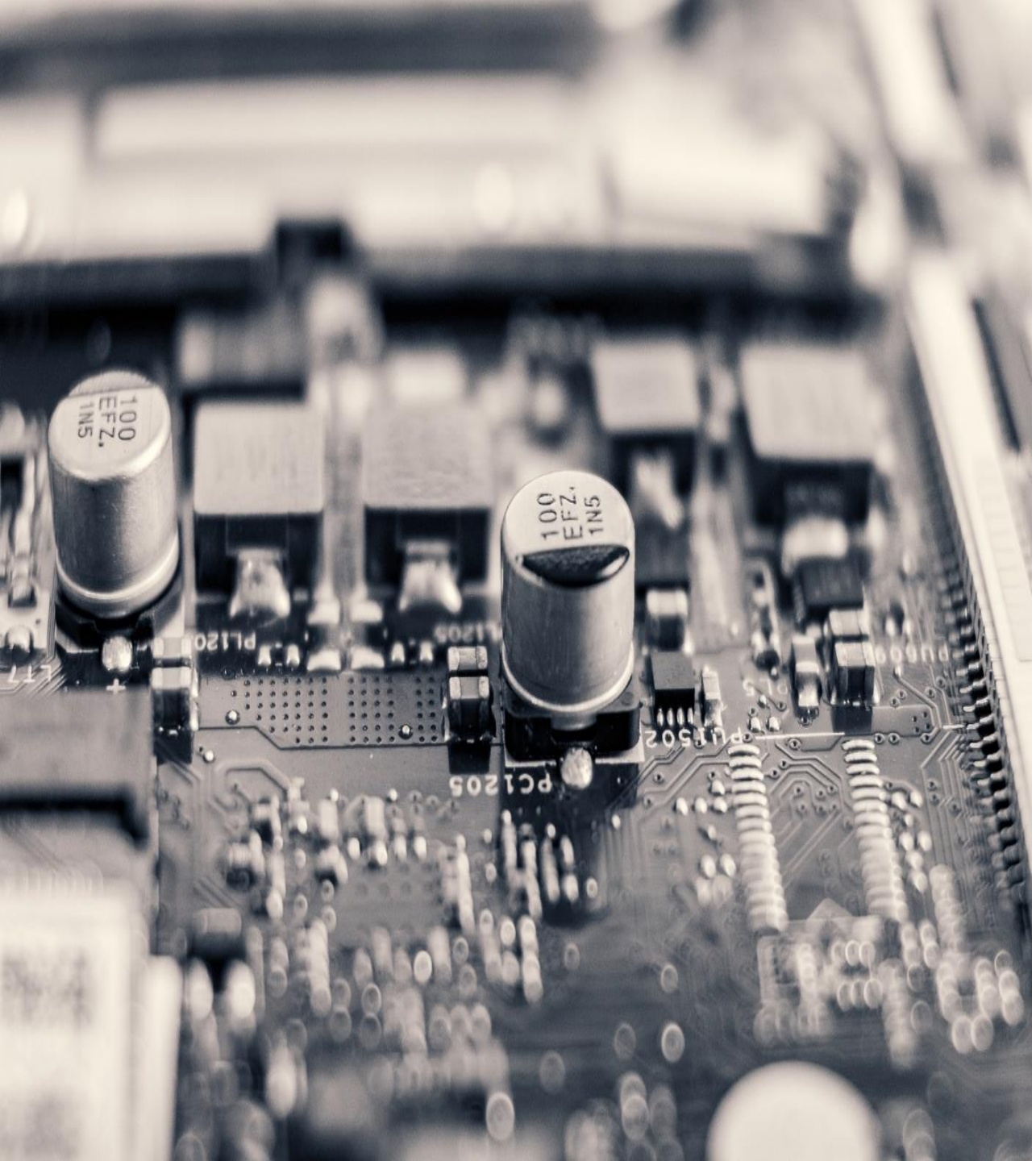
Updates sind ein wichtiger Sicherheitsfaktor:

- **fehlende bzw. nicht eingespielt = Sicherheitslücke**
- **manipulierte = Backdoor etc.**

Gerade für viele der günstig im Netz angebotenen IoT-Gerätschaften gibt es **nach dem Kauf kaum noch oder nur sehr verspätet Updates**, weshalb auch Angriffe auf längst bekannte und „behobene“ Sicherheitslücken oftmals zum Erfolg führen…

<u>Frage:</u> ***Wer hat seine IoT-/Smart-Devices upgedatet bzw. hat sich zumindest darüber informiert???***

Die ESP-Chips bieten neben dem seriellen mit wenigen Code-Zeilen auch ein **OTA-Update (Over The Air)** an. Es wird hierzu ein eigener Access-Point aufgesetzt und über **192.168.4.1** kommt man auf eine Upload-Webseite – seltenst geschützt!!!!



TOP 3 – Unsicheres Eco-System

Wir haben schon einiges gehört was für Möglichkeiten durch die Chips eigentlich vorhanden sind und auch das diese selten genutzt werden.

Unter OWASP Top 3 sind viele Einzelpunkte gelistet – unsicheres Web-Frontend, keine oder geringe Authentifizierung um nur einige zu nennen – aber hier gehören auch die oft auf den Platinen belassenen

- **Zugriffs-/Testpunkte**
- **JTAG bzw. andere**
- **Debug-Interfaces**

die einen (einfachen) Zugriff auf die Flashspeicher oä. erst ermöglichen!

TOP 3 – Unsicheres Eco-System

Möglichkeiten
und auch das

te gelistet –
er geringe
– aber hier
senen

ashspeicher

„Wenn nun ein Krimineller so eine LED-Leuchte vom Grundstück entwendet, in seiner Werkstatt öffnet und mit Spezialgerät und einigen kleinere Lötarbeiten den Speicherchip mit dem darin gespeicherten Passwort ausliest, ist er im Besitz des WLAN-Passwortes.“

Aus „Smart Wohnen 2/2019“

Günther Ohland
VV SmartHome Initiative Deutschland e.V.

TOP 1 – Passwörter

Kaum ein anderer Punkt ist so fest unter den potentiellen Sicherheitsrisiken verwurzelt wie die Passwörter.

Zu kurz, zu einfach, geleaked und trotzdem weitergenutzt…. – die Liste der möglichen Risiken ist *im Gegensatz zu vielen Passwörtern* lang.

Bei IoT- Geräten kommt jedoch der Punkt der Speicherung erschwerend dazu:

Wo legt das Gerät denn die notwendigen WLAN-Zugangsdaten oder User-Kennwörter ab?

- *Im **Flash-Speicher**?*
- *Auf einer **SD- Karte**?*
- *In einer (fremden) **Cloud**?*

Wie leicht man daran kommt haben wir schon gesehen…

Fazit

Für „Otto Normalanwender“, dem Bequemlichkeit vor allem geht und der sich nicht als potentielles Ziel von Hacker sieht, scheint alles gut zu sein **– aber bei vielen der IoT- und Smart-Devices ist „Verbesserungspotential“ in Punkto Sicherheit gegeben!**

Vieles liegt leider aber auch schon bei der Entwicklung im Argen, denn die Chips bieten hardwareseitig schon genug Möglichkeiten um einige der gravierenden Löcher gar nicht erst entstehen zu lassen!

Ich hoffe, ich habe bis zu dieser Folie noch nicht zu lange überzogen - denn

für den sicherheitsbewussten Anwender möchte ich gerne noch ein paar Tipps geben...

Eyes on IoT – Security

Generell gelten auch beim Internet der Dinge **alle grundsätzlichen Sicherheitsregeln wie bei allem anderen IT-Systemen**, jedoch gilt es auch verstärkt sein Augenmerk auf folgende Punkte zu richten:

1. **(Hersteller-)Cloud-basierter Zugriff?**
   - ➔ *Muss ich von überall zugreifen?*
   - ➔ *Alternative Firmware vorhanden?*
2. **Wohin nimmt das Gerät Kontakt auf?**
   - ➔ *Kurzer Check mit RASPION/ PIHOLE*
     - ➔ *Nach Blacklisten noch funktionsfähig???*
   - ➔ *Undokumentierte Port-Listener eingerichtet?*
     - ➔ *per Portscan überprüfen*
3. **Gibt es (weiterhin) Updates für das Gerät?**
4. **Generell alle Grundeinstellungen überprüfen und auf eigene Bedürfnisse anpassen**
5. **KEINE Original-/Standardzugangsdaten verwenden!**
6. **Netzwerk segmentieren (evtl. kein Gastnetz nutzbar)**

Ein herzliches Dankeschön das ich bei Ihnen diesen Vortrag* halten durfte!

Frank Ewert

EDU cation
SECU rity
IT

frank.ewert@edu-secu-it.de

*** Diese Präsentation und ein Handout mit Tipps etc. (RaSpion/ PiHole etc.) stelle ich Dieter Carbon in den nächsten Tagen zur Verfügung!**